2023. évi XXIII. törvény

a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

A társadalom gyors digitális átalakulásával és összekapcsolódásával az elektronikus információs rendszerek, valamint a digitális eszközök a mindennapi élet központi elemévé váltak. A fejlődés a digitális fenyegetettségek körének bővüléséhez is vezetett, ami akadályozhatja a gazdasági tevékenységek folytatását, pénzügyi veszteséget okozhat és alááshatja a felhasználók bizalmát, ezzel jelentős károkat okozva a gazdasági és társadalmi életben. Ezen túlmenően a kiberbiztonság kulcsfontosságú tényező számos kritikus ágazat számára a digitális átalakulás sikeres felkarolásához és a digitalizáció gazdasági, társadalmi és fenntartható előnyeinek teljes körű kiaknázásához. Mindezekre figyelemmel az Országgyűlés a következő törvényt alkotja:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. § E törvény alkalmazásában:

1. *adatközponti szolgáltatás:* olyan szolgáltatás, amely központosított elhelyezést, összeköttetést és működést biztosít adattároló, -feldolgozó és -továbbító információtechnológiai és hálózati berendezések számára, ideértve az energiaellátást és környezeti felügyeletet biztosító létesítményeket és infrastruktúrát is,

2. *behatolásvizsgálat:* az információs és kommunikációs technológia (a továbbiakban: IKT) rendszer, valamint az elektronikus információs rendszer gyenge pontjainak feltárása és kihasználhatóságának ellenőrzése a biztonsági intézkedések elleni rosszindulatú támadások szimulációjával,

3. *belső informatikai biztonsági vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során az informatikai rendszer sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik,

4. *bizalmasság:* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

5. *biztonsági esemény:* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

6. *DNS-szolgáltató:* olyan szervezet, amely a következő szolgáltatások valamelyikét nyújtja:

a) autoritatív DNS-szolgáltatás: a domainnév – domainnév-regisztrációt végző szolgáltató által kezelt – adatainak lekérdezését közvetlenül lehetővé tevő szolgáltatás, amely a legfelső szintű domainnév-nyilvántartó szolgáltatás része,

b) rekurzív DNS-szolgáltatás: olyan DNS-szolgáltatás, amely a felhasználók domainnév-lekérdezéseit a megfelelő autoritatív DNS-szolgáltatókhoz továbbítja a hierarchikusan felépülő domainnévrendszerben és az autoritatív DNS-szolgáltató által a lekérdezésre adott válaszokat továbbítja a felhasználó részére,

c) DNS-gyorsítótárazás: a domainnév-lekérdezésre adott válaszok átmeneti tárolása és a felhasználói lekérdezéseknek a tárolt domainnévadatok alapján történő kiszolgálása,

7. *domainnév:* az internetes kommunikációhoz használt IP-cím alfanumerikus karakterekből álló megfelelője,

8. *domainnév-regisztrációt végző szolgáltató:* a legfelső szintű domainnév-nyilvántartó által felhatalmazott szolgáltató, amely jogosult domain regisztrálására,

9. *elektronikus információs rendszer:* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

10. *európai kiberbiztonsági tanúsítási rendszer:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 9. pontja szerinti rendszer,

11. *felhőalapú számítástechnikai szolgáltatás:* olyan digitális szolgáltatás, amely önkiszolgáló módon történő hálózati hozzáférést tesz lehetővé igény szerint méretezhető, megosztott fizikai vagy virtuális erőforrások rugalmas készletéhez,

12. *felhőszolgáltató:* felhőalapú számítástechnikai szolgáltatást nyújtó szervezet,

13. *gyártó:* az IKT-termék gyártója, IKT-szolgáltatás nyújtója, valamint IKT-folyamat gyártója vagy nyújtója,

14. *IKT-folyamat:* az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

15. *IKT-szolgáltatás:* az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

16. *IKT-termék:* az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

17. *kiberbiztonsági audit:* az elektronikus információs rendszerek tekintetében a kiberbiztonsági követelmények teljesülésére vonatkozó vizsgálat, ellenőrzés,

18. *kiberfenyegetés:* az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

19. *kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató:* olyan kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, amely a kiberbiztonsági kockázatok kezelését végzi vagy azzal összefüggő szolgáltatást nyújt,

20. *kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató:* olyan szervezet, amely az IKT-termék, hálózat, infrastruktúra, alkalmazás vagy bármely más elektronikus információs rendszer telepítésével, kezelésével, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt a szolgáltatást igénybe vevő telephelyén vagy távolról,

21. *közösségimédia-szolgáltatási platform:* olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg, fedezzenek fel és kommunikáljanak egymással,

22. *kutatóhely:* a tudományos kutatásról, fejlesztésről és innovációról szóló törvény szerinti kutatóhely – az oktatási intézmények kivételével –, amelynek elsődleges célja alkalmazott kutatás vagy kísérleti fejlesztés folytatása a kutatás eredményeinek kereskedelmi célokra való hasznosítása céljából,

23. *legfelső szintű domainnév-nyilvántartó:* olyan szervezet, amelyre egy meghatározott legfelső szintű domaint bíztak és amely felelős egyrészt a legfelső szintű domain kezeléséért – ideértve a legfelső szintű domain alatti domainnevek nyilvántartásba vételét –, másrészt a legfelső szintű domain technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a legfelső szintű domainzónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezeknek az üzemeltetési tevékenységeknek bármelyikét maga a szervezet végzi vagy azokat kiszervezi, kivéve azokat az eseteket, amikor a legfelső szintű domainneveket a nyilvántartó kizárólag saját használatra veszi igénybe,

24. *megfelelőségértékelés:* az az értékelési eljárás, amely bizonyítja, hogy egy IKT-termékkel, IKT-folyamattal, IKT-szolgáltatással kapcsolatos, meghatározott követelmények teljesültek,

25. *megfelelőségértékelő szervezet:* a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló, 2008. július 9-i 765/2008/EK európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

26. *megfelelőségi nyilatkozat:* a gyártó vagy a szolgáltató által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek,

27. *megfelelőségi önértékelés:* az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként

meghatározott fogalom,

28. *nemzeti kiberbiztonsági tanúsítási rendszer:* IKT-termékek, IKT-szolgáltatások és IKT-folyamatok tanúsítására, megfelelőségértékelésére Magyarországon alkalmazandó, az európai kiberbiztonsági rendszerek elvei alapján kidolgozott és a tanúsító hatóság által meghatározott szabályok, műszaki követelmények, szabványok és eljárások átfogó rendszere,

29. *nemzeti kiberbiztonsági tanúsítvány:* olyan független harmadik fél által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek,

30. *online piactér:* olyan szolgáltatás, amely a kereskedő által vagy a kereskedő nevében működtetett szoftvert, többek között weboldalt, valamely weboldal egy részét vagy valamely alkalmazást alkalmaz, és amelynek révén a fogyasztók távollevők közötti szerződést köthetnek más kereskedőkkel vagy fogyasztókkal,

31. *rendelkezésre állás:* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

32. *sértetlenség:* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

33. *tanúsítás:* független harmadik fél által végzett megfelelőségértékelési tevékenység,

34. *tartalomszolgáltató hálózat szolgáltatója:* a digitális tartalmak és szolgáltatások széles körű, akadálymentes és gyors rendelkezésre állását biztosító, földrajzilag elosztott szerverek hálózatának szolgáltatója,

35. *távoli sérülékenységvizsgálat:* olyan informatikai biztonsági vizsgálat, amelynek során

a) az elektronikus információs rendszer internet felőli, külső sérülékenységvizsgálatára kerül sor, amelynek keretében az interneten fellelhető, nyilvános adatbázisokban való szabad keresés, célzott információgyűjtés, valamint az elérhető számítógépek szolgáltatásai sebezhetőségének feltérképezése történik,

b) automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei, vagy

c) a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik.

2. § Az e törvény hatálya alá tartozó hatósági eljárásokban az általános közigazgatási rendtartásról szóló törvény rendelkezéseit az e törvényben, a fogyasztóvédelemről szóló törvényben, a termékek piacfelügyeletéről szóló törvényben és a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló törvényben foglalt eltérésekkel és kiegészítésekkel, valamint a polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről szóló kormányrendeletben és a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) elnöke által kiadott rendeletben foglalt kiegészítésekkel kell alkalmazni.

II. FEJEZET

TANÚSÍTÁSI RENDSZEREK

1. A tanúsító hatóság feladatai

3. § (1) Az e fejezetben foglaltakat IKT-termék, IKT-szolgáltatás vagy IKT-folyamat tanúsításával kapcsolatos hatósági tevékenységre kell alkalmazni.

(2) Az e fejezetben szabályozott kiberbiztonsági tanúsításra, valamint a tanúsító szervezet tevékenységére nem kell alkalmazni a megfelelőségértékelő szervezetek tevékenységéről szóló

törvény rendelkezéseit.

4. § (1) Az (EU) 2019/881 európai parlamenti és tanácsi rendelet szerinti nemzeti kiberbiztonsági tanúsító hatóság (a továbbiakban: tanúsító hatóság) feladatait

a) – a *b)* pont kivételével – az SZTFH,

b) a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében a Kormány által kijelölt hatóság

látja el.

(2) A hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a nemzeti kiberbiztonsági tanúsítási rendszereket az SZTFH elnöke rendeletben határozza meg. A hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a nemzeti kiberbiztonsági tanúsítási rendszerekre figyelemmel a tanúsítási rendszereket a Kormány rendeletben határozza meg.

5. § (1) A tanúsító hatóság az európai kiberbiztonsági tanúsítási rendszerekkel kapcsolatosan

a) nyomon követi az európai kiberbiztonsági tanúsítási rendszerek fejlesztését és figyelemmel kíséri a kapcsolódó szabványosítási folyamatokat,

b) részt vesz az európai kiberbiztonsági tanúsítási csoport tevékenységében,

c) információkat gyűjt azokról az ágazatokról és szakterületekről, amelyek nem esnek európai kiberbiztonsági tanúsítási rendszer hatálya alá és amelyek esetében a kiberbiztonság növelése szükséges,

d) az érdekelt feleknek szükség esetén tájékoztatást, támogatást nyújt,

e) elvégzi az (EU) 2019/881 európai parlamenti és tanácsi rendelet 57. cikk (4) bekezdése szerinti tájékoztatást.

(2) A tanúsító hatóság a nemzeti kiberbiztonsági tanúsítási rendszerek fenntartásával kapcsolatosan

a) legalább háromévente, az aktuális biztonsági kockázatokra figyelemmel értékeli a hatályos nemzeti kiberbiztonsági tanúsítási rendszereket,

b) felülvizsgálatot megalapozó ok felmerülését követően haladéktalanul intézkedik a nemzeti kiberbiztonsági tanúsítási rendszer felülvizsgálata érdekében,

c) európai kiberbiztonsági tanúsítási rendszer kiadása esetén haladéktalanul intézkedik az azonos tárgyú nemzeti kiberbiztonsági tanúsítási rendszer felülvizsgálata, továbbá hatályon kívül helyezése érdekében.

(3) Az (1) bekezdés *b)* és *e)* pontja szerinti feladatok tekintetében tanúsító hatóságként az SZTFH jár el.

2. A nemzeti kiberbiztonsági tanúsítási rendszerek követelményei

6. § A nemzeti kiberbiztonsági tanúsítási rendszernek a következő biztonsági célokat kell teljesítenie:

a) a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan tárolással, kezeléssel, hozzáféréssel és közléssel szemben az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt,

b) a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan megsemmisítéssel, elvesztéssel, megváltoztatással vagy a hozzáférhetetlenséggel szemben az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt,

c) annak biztosítása, hogy a feljogosított személyek, programok vagy gépek kizárólag a hozzáférési jogaik tárgyát képező adatokhoz, szolgáltatásokhoz vagy funkciókhoz férhetnek hozzá,

d) az ismert függőségek és sebezhetőségek azonosítása és dokumentálása,

e) annak rögzítése, hogy a feljogosított személy, program vagy gép mely időpontban és mely védendő adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy egyéb módon kezelt,

f) annak ellenőrizhetővé tétele, hogy a feljogosított személy, program vagy gép mely időpontban és mely adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy egyéb módon kezelt,

g) annak ellenőrzése, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok nem tartalmaznak-e ismert sebezhetőségeket,

h) fizikai vagy műszaki biztonsági esemény bekövetkeztekor az adatok, a szolgáltatások és a funkciók rendelkezésre állásának, valamint az adatokhoz, a szolgáltatásokhoz és a funkciókhoz való hozzáférésnek a mihamarabbi helyreállítása,

i) annak biztosítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok kockázatarányosan, alapértelmezetten és tervezetten biztonságosak legyenek,

j) annak biztosítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok szoftvere és hardvere naprakész legyen, és

k) annak biztosítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok vonatkozásában nem állnak fenn közismert sebezhetőségek, továbbá rendelkezésre állnak a biztonságos frissítésükre szolgáló mechanizmusok.

7. § (1) A nemzeti kiberbiztonsági tanúsítási rendszernek tartalmaznia kell:

a) a tanúsítási rendszer tárgyát és hatályát, az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok típusát vagy kategóriáit,

b) a tanúsítási rendszer céljának és annak az egyértelmű meghatározását, hogy a kiválasztott szabványok, értékelési módszerek és megbízhatósági szintek milyen módon felelnek meg a rendszer célfelhasználói igényeinek,

c) hivatkozást az értékelésben alkalmazott nemzetközi, európai vagy nemzeti szabványokra, vagy ha nem állnak rendelkezésre ilyen szabványok vagy azok nem megfelelőek, az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendelet II. mellékletében meghatározott követelményeket teljesítő műszaki előírásokra, vagy ha ilyen előírások nem állnak rendelkezésre, az európai kiberbiztonsági tanúsítási rendszerben meghatározott műszaki előírásra vagy egyéb kiberbiztonsági követelményekre való hivatkozást,

d) a megbízhatósági szintet vagy szinteket,

e) a megfelelőségi önértékelésre vonatkozó kizáró vagy megengedő rendelkezést,

f) a megfelelőségértékelést végző személyekre, szervezetekre alkalmazandó kiegészítő követelményeket,

g) az alkalmazandó konkrét értékelési kritériumokat és módszereket, ideértve az értékelés típusait is,

h) a jelölések vagy címkék használati feltételeit,

i) a kiadandó nemzeti kiberbiztonsági tanúsítvány vagy megfelelőségi nyilatkozat tartalmát és formátumát, és

j) a rendszer alapján kibocsátott nemzeti kiberbiztonsági tanúsítványok kibocsátására, érvényességi idejére, fenntartására, meghosszabbítására, megújítására, valamint a hatályának bővítésére vagy szűkítésére vonatkozó feltételeket.

(2) Ha a nemzeti kiberbiztonsági tanúsítási rendszer több megbízhatósági szintre is érvényes, akkor a követelményeknek tartalmazniuk kell a különböző megbízhatósági szintekre vonatkozó elvárások pontos megkülönböztetését.

(3) A nemzeti kiberbiztonsági tanúsítási rendszerben meg kell határozni

a) az egyes követelményekhez vagy követelmény csoportokhoz tartozó értékelési eljárásokat,

b) azokat a kritikus védelmi funkciókat, amelyek esetében végre kell hajtani a tevékenység utólagos nyomon követésére is alkalmas belső informatikai biztonsági vagy távoli sérülékenységvizsgálatot vagy behatolásvizsgálatot, kriptográfiai értékeléseket, biztonsági forráskód-elemzéseket, valamint

c) az értékelési eredmények dokumentálására vonatkozó követelményeket.

3. A nemzeti kiberbiztonsági tanúsítási rendszerek megbízhatósági szintjei

8. § (1) A nemzeti kiberbiztonsági tanúsítási rendszerek az IKT-termékekre, az IKT-szolgáltatásokra és az IKT-folyamatokra az „alap”, a „jelentős” és a „magas” megbízhatósági szintek közül egy vagy több szintet határozhatnak meg.

(2) A megbízhatósági szint arra vonatkozóan szolgál biztosítékkal, hogy az adott IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok teljesítik a vonatkozó biztonsági követelményeket, biztonsági funkciókat és olyan szintű értékelésen estek át, amely

a) „alap” megbízhatósági szinten a biztonsági eseményekkel és támadásokkal kapcsolatos alapvető, ismert kockázatok,

b) „jelentős” megbízhatósági szinten az ismert kiberbiztonsági kockázatok, valamint a korlátozott szakértelemmel és erőforrásokkal rendelkező elkövetők által végrehajtott biztonsági események és kiberbiztonsági támadások kockázatának,

c) „magas” megbízhatósági szinten a jelentős szakértelemmel és erőforrásokkal rendelkező elkövetők által, a tudomány legutolsó állása szerinti technológiával végrehajtott kibertámadások kockázatának
minimalizálására törekszik.

(3) A megbízhatósági szintnek a biztonsági események valószínűsége és hatása szempontjából arányban kell állnia az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat rendeltetés szerinti használatához kapcsolódó kockázat szintjével.

(4) Az elvégzendő értékelési tevékenységeknek legalább a következőket kell magukban foglalniuk:

a) „alap” megbízhatósági szint esetén a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,

b) „jelentős” megbízhatósági szint esetén

ba) a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,

bb) a közismert sebezhetőségek hiánya megállapításának felülvizsgálatát, és

bc) az annak megállapítására szolgáló tesztelést, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelelően működteti-e a szükséges biztonsági funkciókat,

c) „magas” megbízhatósági szint esetén

ca) a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,

cb) a közismert sebezhetőségek hiánya megállapításának felülvizsgálatát,

cc) az annak megállapítására szolgáló tesztelést, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelelően, a legfejlettebb technika szerint működteti-e a szükséges biztonsági funkciókat, valamint

cd) behatolásvizsgálatok révén annak értékelését, hogy az mennyire ellenálló a jól képzett elkövetők által végrehajtott támadásokkal szemben.

4. A kiberbiztonsági tanúsítványokkal és a megfelelőségi nyilatkozatokkal kapcsolatos elvárások

9. § (1) A nemzeti kiberbiztonsági tanúsítványban és a nemzeti megfelelőségi nyilatkozatban meg kell jelölni:

a) azt a nemzeti kiberbiztonsági tanúsítási rendszert, amely alapján a tanúsítvány vagy a nyilatkozat kiállításra került,

b) a megbízhatósági szintet, valamint

c) a vonatkozó műszaki előírásokat, szabványokat és eljárásokat.

(2) A nemzeti kiberbiztonsági tanúsítványban és a nemzeti megfelelőségi nyilatkozatban fel kell tüntetni:

a) a kiállító szervezet nevét, címét,

b) a kiállítás dátumát,

c) a gyártó nevét és címét,

d) a megfelelőségértékelés megbízóját,

e) az alkalmazási területeket, vagy ha az adott alkalmazási területeken a megfelelőség feltételekkel érvényes, ezen feltételeket,

f) az érvényességi időt,

g) a tanúsítás tárgyát képező IKT-termék, IKT-szolgáltatás és IKT-folyamat azonosítását, ha van, annak verziószámát, valamint

h) a kiállító aláírását.

(3) A tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat gyártója vagy az olyan IKT-termék, IKT-szolgáltatás vagy IKT-folyamat gyártója, amelynek tekintetében megfelelőségi nyilatkozatot állítottak ki, köteles az IKT-termék, IKT-szolgáltatás vagy IKT-folyamat biztonságát érintő sebezhetőségről vagy rendellenességről haladéktalanul tájékoztatni a tanúsító hatóságot.

10. § (1) Azon az IKT-terméken, IKT-szolgáltatáson vagy IKT-folyamatban, amely tanúsított, vagy amelynek tekintetében megfelelőségi nyilatkozatot állítottak ki, – az SZTFH elnökének vagy a 4. § (1) bekezdés *b)* pontja szerinti esetben a Kormány rendeletében meghatározott módon – nemzeti vagy európai kiberbiztonsági tanúsítási rendszer által előírt formában megfelelőségi jelölést kell elhelyezni.

(2) Tilos az (1) bekezdés szerinti megfelelőségi jelölés jogosulatlan elhelyezése, valamint olyan jelölés elhelyezése, amely hasonlít a megfelelőségi jelölés formájára, vagy azt a látszatot kelti, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat tanúsított, vagy annak vonatkozásában megfelelőségi nyilatkozatot állítottak ki, és így harmadik felet megtéveszthet.

5. Megfelelőségi önértékelés, megfelelőségértékelés

11. § (1) Megfelelőségi önértékelésre abban az esetben kerülhet sor, ha azt a nemzeti kiberbiztonsági tanúsítási rendszer az „alap” megbízhatósági szintnek megfelelő, alacsony kockázatot jelentő IKT-termékek, IKT-szolgáltatások és IKT-folyamatok esetében lehetővé teszi.

(2) A gyártó nemzeti megfelelőségi nyilatkozatot állít ki arról, hogy megtörtént annak vizsgálata, hogy a nemzeti kiberbiztonsági tanúsítási rendszer követelményei teljesülnek. A vizsgálatnak tartalmaznia kell a nemzeti kiberbiztonsági tanúsítási rendszer követelményei teljesülésének a tanúsítási rendszerben meghatározott módszertan szerinti értékelését.

(3) A megfelelőségi önértékelést végző gyártó a (2) bekezdés szerinti megfelelőségi nyilatkozat kiállítását követő 15 napon belül, nyilvántartásba vétel céljából – elektronikusan kereshető formában is – megküldi a tanúsító hatóság részére a megfelelőségi nyilatkozat másolati példányát, a műszaki dokumentációt, a nemzeti kiberbiztonsági tanúsítási rendszerben meghatározott értékelési módszer alapján elkészített értékelési jelentést, valamint a megjelölt tanúsítási rendszernek való megfeleléssel kapcsolatos összes egyéb lényeges értékelési információt.

12. § Harmadik fél által végzett megfelelőségértékelési tevékenységet csak olyan szervezet végezhet,

a) amelyet a vonatkozó nemzeti vagy európai kiberbiztonsági tanúsítási rendszerben meghatározott követelményekre figyelemmel a nemzeti akkreditálásról szóló törvény szerint kijelölt akkreditáló szerv akkreditált vagy külföldi akkreditált státusz esetén e státuszát elismerte,

b) amely az SZTFH elnökének rendeletében az egyes megbízhatósági szintekre vonatkozóan meghatározott követelményeknek megfelel, és

c) amelyet a tanúsító hatóság nyilvántartásba vett.

6. A kiberbiztonsági tanúsítás felügyelete

13. § (1) A tanúsító hatóság eljárása során a sommás eljárás kizárt.

(2) A tanúsító hatóság ügyintézési határideje 120 nap.

(3) Európai kiberbiztonsági tanúsítási rendszer esetében a tanúsító hatóság a nemzeti akkreditáló szerv által akkreditált megfelelőségértékelő szervezetet a hatósági nyilvántartásba vételről szóló határozat véglegessé válásától számított 15 napon belül bejelenti az Európai Bizottság (a továbbiakban: Bizottság) részére. A kérelmező szervezet az akkreditált státuszát a nemzeti akkreditáló szerv határozatának csatolásával igazolja.

(4) A tanúsító hatóság a megfelelőségértékelő szervezet vonatkozásában engedélyezési eljárást folytat le, ha az IKT-termékre, IKT-szolgáltatásra vagy IKT-folyamatra vonatkozó nemzeti vagy európai kiberbiztonsági tanúsítási rendszer

a) kiegészítő követelményeket ír elő és ez alapján engedélyezési eljárás lefolytatása válik szükségessé, vagy

b) „magas” megbízhatósági szintet ír elő a rendszer keretében kiadandó kiberbiztonsági tanúsítványra és a tanúsító hatóság az ilyen tanúsítvány kiállításának feladatát egyes nemzeti vagy európai kiberbiztonsági tanúsítványok vonatkozásában vagy általános jelleggel átruházza a megfelelőségértékelő szervezetre.

(5) A (4) bekezdés *b)* pontja szerinti esetben az engedély megadásának feltétele, hogy a megfelelőségértékelő szervezet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti, a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetnek minősüljön.

(6) A (4) bekezdés szerinti engedély hatálya legfeljebb az akkreditált státusz lejártáig terjedhet.

(7) Európai kiberbiztonsági tanúsítási rendszer esetében a tanúsító hatóság a (4) bekezdés szerinti engedélyezési eljárás lefolytatása esetén a megfelelőségértékelő szervezetet az engedély megadásáról szóló határozat véglegessé válását követő 15 napon belül bejelenti a Bizottságnak.

(8) A tanúsító hatóság kiberbiztonsági tanúsítási felügyeleti feladatai keretében jogosult

a) felszólítani a megfelelőségértékelő szervezeteket és a megfelelőségi nyilatkozatok kibocsátóit a hatósági feladatellátáshoz szükséges információk, adatok rendelkezésre bocsátására, valamint

b) a megfelelőségértékelő szervezeteknél és a megfelelőségi nyilatkozatok kibocsátóinál hatósági ellenőrzést végezni.

(9) Az egyes tanúsító hatósági eljárásokért igazgatási szolgáltatási díjat kell fizetni. Az igazgatási szolgáltatási díj mértékét és az annak beszedésével, megosztásával, kezelésével, nyilvántartásával és visszatérítésével kapcsolatos részletes szabályokat

a) a 4. § (1) bekezdés *a)* pontja szerinti tanúsító hatóság által lefolytatott eljárások esetében az SZTFH elnökének a nemzeti kiberbiztonsági tanúsító hatóság eljárásával összefüggő kiberbiztonsági tanúsítás keretében fizetendő igazgatási szolgáltatási díjról szóló rendelete,

b) a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság által lefolytatott eljárások esetében az e törvény végrehajtására kiadott miniszteri rendelet

határozza meg.

14. § (1) A tanúsító hatóság nyilvántartja és kezeli:

a) az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártója által rendelkezésre bocsátott megfelelőségi nyilatkozat adatait,

b) a megfelelőségi nyilatkozathoz benyújtott műszaki dokumentációt és az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok tanúsítási rendszernek való megfelelésével kapcsolatos információkat,

c) a megfelelőségértékelő szervezet és annak kijelölt kapcsolattartója azonosításához szükséges adatokat, ha a megfelelőségértékelő szervezet egyben az (EU) 2019/881 európai parlamenti és tanácsi rendelet 56. cikk (5) bekezdése szerinti közjogi szerv, ennek tényét, valamint az SZTFH elnökének rendeletében meghatározott követelmények teljesülését alátámasztó dokumentumokat,

d) a nemzeti akkreditáló szerv által akkreditált megfelelőségértékelő szervezet akkreditált státuszára vonatkozó határozatban foglalt, valamint az akkreditált státusz változására vonatkozó információkat,

e) ha a 13. § (4) bekezdése szerinti engedélyezési eljárás lefolytatása szükséges, akkor az azzal kapcsolatos kérelmet, adatokat és dokumentumokat,

f) az engedélyezési eljárás során kiadott engedélyre, annak felfüggesztésére, részben vagy egészben történő visszavonására vonatkozó adatokat, valamint annak tényét, hogy az engedély hatályát vesztette,

g) ha a tanúsító hatóság a „magas” megbízhatósági szintű kiberbiztonsági tanúsítvány kiállításának jogát megfelelőségértékelő szervezetre átruházta, a delegált jogkör azonosításához szükséges adatokat,

h) a Bizottság által a megfelelőségértékelő szervezet nyilvántartásba vételekor adott azonosító számot,

i) a megfelelőségértékelő szervezet által igénybe vett közreműködő, valamint kijelölt kapcsolattartója azonosításához szükséges adatokat,

j) a megfelelőségértékelő szervezet által kiadott tanúsítvány adatait,

k) a gyártó, valamint kijelölt kapcsolattartója azonosításához szükséges adatokat,

l) a tanúsítványok kiállításának megtagadásával, hatályának korlátozásával, felfüggesztésével és a visszavonásával kapcsolatos információkat,

m) a 9. § (3) bekezdése szerinti sebezhetőséggel vagy rendellenességgel kapcsolatos információt,

n) a felügyeleti tevékenység ellátása során tudomására jutott adatokat, dokumentumokat, valamint

o) a benyújtott panaszokkal kapcsolatos adatokat, dokumentumokat.

(2) Az (1) bekezdés szerinti nyilvántartás az (1) bekezdés *f)* és *g)* pontja szerinti adatok tekintetében közhiteles nyilvántartásnak minősül.

(3) Az (1) bekezdés szerinti adatok kezelésének célja az IKT-termék, IKT-szolgáltatás vagy IKT-folyamat biztonságával összefüggő információk naprakészen tartása, valamint az azokat érintő sebezhetőséggel vagy rendellenességgel kapcsolatos feladatok, továbbá a tanúsító hatóság ellenőrzési és felügyeleti hatósági tevékenységének ellátása.

(4) Az (1) bekezdés szerinti nyilvántartásban szereplő bármely adatot érintően – ha jogszabály eltérően nem rendelkezik – a következő szervezetek részére végezhető adattovábbítás:

a) a Bizottság részére a bejelentett megfelelőségértékelő szervezetek jegyzékének összeállítása és frissítése,

b) a nemzeti akkreditálásról szóló törvény szerint kijelölt akkreditáló szerv részére a megfelelőségértékelő szervezetek tevékenységének akkreditációjával és felügyeletével kapcsolatos feladatok ellátása, valamint

c) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti eseménykezelő központok részére a 9. § (3) bekezdése szerinti sebezhetőséggel vagy rendellenességgel kapcsolatos tevékenység ellátása

érdekében.

(5) A megfelelőségértékelő szervezet és a gyártó az (1) bekezdés szerinti adatokat az adatok rendelkezésre állásától, valamint az adatok változását a változás bekövetkezésétől számított 8 napon belül megküldi a tanúsító hatóság részére a nyilvántartásba vétel érdekében.

15. § (1) Ha a tanúsító hatóság tudomására jut vagy az ellenőrzése során megállapítja, hogy a megfelelőségértékelő szervezet vagy a gyártó a vonatkozó európai uniós vagy magyar jogszabályokban foglalt biztonsági követelményeket és a kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, – a figyelmeztetést tartalmazó döntésében határidő tűzésével – felszólítja a megfelelőségértékelő szervezetet vagy a gyártót a vonatkozó európai uniós és magyar jogszabályokban foglalt biztonsági követelmények és a kapcsolódó eljárási szabályok teljesítésére.

(2) Ha az (1) bekezdésben meghatározottak ellenére a megfelelőségértékelő szervezet vagy a gyártó a jogszabályban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a tanúsító hatóság – az eset összes körülményének mérlegelésével, kormányrendeletben meghatározottak szerint – bírságot szabhat ki, amely további nemteljesítés esetén megismételhető.

16. § (1) A tanúsító hatóság a feladatellátása során megismert minősített adatot, személyes adatot vagy különleges adatot, valamint az üzleti titoknak, banktitoknak, fizetési titoknak, biztosítási titoknak, értékpapírtitoknak, pénztártitoknak, orvosi titoknak és más hivatás gyakorlásához kötött

titoknak minősülő és törvény által védett egyéb adatot kizárólag a feladat ellátásának időtartama alatt, a célhoz kötöttség elvének figyelembevételével kezeli. A tanúsító hatóság a hatósági ellenőrzés eredményeként tett megállapításokat alátámasztó adatokat rögzíti, és az így rögzített adatokat a megfelelőségértékelő szervezet akkreditált státuszának megszűnését követő 10. év utolsó napjáig, vagy a gyártó által kiadott megfelelőségi nyilatkozat hatályosságának megszűnését követő 10. év utolsó napjáig kezeli azzal, hogy ha az ellenőrzéssel érintett IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében megfelelőségértékelő szervezet által kiadott tanúsítvány és megfelelőségi önértékelés is rendelkezésre áll, az akkreditált státusz megszűnésének és a megfelelőségi nyilatkozat hatályossága megszűnésének időpontja közül a későbbi időpontot kell figyelembe venni. Ezt követően a tanúsító hatóság az adatokat az elektronikus információs rendszereiből és adathordozóiról törli.

(2) A tanúsító hatóság eljárása során keletkezett adatok – ha törvény eltérően nem rendelkezik – nem nyilvánosak.

(3) A tanúsító hatóság munkatársait az (1) bekezdés szerint megismert adatok tekintetében – a jogszabályban meghatározott kivételekkel – titoktartási kötelezettség terheli, amely a foglalkoztatásra irányuló jogviszony megszűnését követő 5 évig, minősített adatok tekintetében azok érvényességi idejének végéig, személyes adatok tekintetében pedig időkorlát nélkül fennmarad.

(4) A tanúsító hatóság a tanúsító hatósági tevékenységét, a hatósági ellenőrzést, valamint a nyilvántartás vezetésével kapcsolatos feladatainak ellátását az SZTFH elnöke – a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság tekintetében a Kormány – rendeletében foglaltak szerint végzi.

(5) A gyártó a megfelelőségi önértékelés során, valamint a megfelelőségértékelő szervezet a tanúsítási eljárás során az SZTFH elnöke – a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság tekintetében a Kormány – rendeletében foglaltak szerint jár el.

III. FEJEZET

KIBERBIZTONSÁGI FELÜGYELET

7.

17–18. §

8. Alapvető követelmények

19. §
20. §
21. §

9. Kiberbiztonsági felügyeleti eszközök

22. § (1)
(2)–(5)
(6)
(7)–(9)
23. § (1)
(2)
(3)

(4)
(5)
(6)
(7)
(8)–(10)
(11)
(12)
(13)
24. §
25. §
26. §

10.

27. §

IV. FEJEZET

ZÁRÓ RENDELKEZÉSEK

11. Felhatalmazó rendelkezések

28. § (1) Felhatalmazást kap a Kormány, hogy rendeletben meghatározza

a) a tanúsító hatóság által kiszabható bírság mértékét, megállapításának szempontrendszerét, valamint a bírság megfizetése módjának részletes eljárási szabályait,

b) a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság feladatának, a tanúsító hatósági tevékenység eljárásrendjének, az engedélyezési eljárásnak, a hatósági ellenőrzésnek, a nyilvántartás vezetésének részletes szabályait, valamint a nyilvántartás személyes adatot nem tartalmazó adattartalmát, valamint a megfelelőségi jelölés elhelyezésére vonatkozó szabályokat,

c) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a megfelelőségi önértékelésre, a tanúsítási eljárásra, valamint a megfelelőségértékelő szervezetek kötelezettségeire és tevékenységére vonatkozó részletes szabályokat,

d) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a nemzeti kiberbiztonsági tanúsítási rendszerekre figyelemmel a tanúsítási rendszereket,

e)–g)

(2) Felhatalmazást kap a Kormány, hogy rendeletben kijelölje a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóságot.

(3) Felhatalmazást kap az SZTFH elnöke, hogy rendeletben meghatározza

a) a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatósági tevékenység kivételével a tanúsító hatósági tevékenység eljárásrendjének, az engedélyezési eljárásnak, a hatósági ellenőrzésnek, a nyilvántartás vezetésének részletes szabályait és a nyilvántartás személyes adatot nem tartalmazó adattartalmát, valamint a megfelelőségi jelölés elhelyezésére vonatkozó szabályokat,

b) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a megfelelőségi önértékelésre, a tanúsítási eljárásra, a megfelelőségértékelő szervezetekkel szemben támasztott követelményekre, valamint a megfelelőségértékelő szervezetek kötelezettségeire és azok tevékenységére vonatkozó részletes szabályokat,

c) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a nemzeti kiberbiztonsági tanúsítási rendszereket,

d)
e)
f)
g)
h)
i)
j)

(4) Felhatalmazást kap a honvédelemért felelős miniszter, hogy rendeletben meghatározza

a) az adópolitikáért felelős miniszterrel egyetértésben a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság eljárásáért fizetendő igazgatási szolgáltatási díj mértékét, a díjak beszedésével, megosztásával, kezelésével, nyilvántartásával és visszatérítésével kapcsolatos részletes szabályokat, valamint

b) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a megfelelőségértékelő szervezetekkel szemben támasztott követelményeket.

(5)
(6)

12. Hatályba léptető rendelkezések

29. § (1) Ez a törvény – a (2)–(4) bekezdésben foglalt kivétellel – a kihirdetését követő 8. napon lép hatályba.

(2) A 15. § és a 28. § (1) bekezdés *a)* pontja az e törvény kihirdetését követő 16. napon lép hatályba.

(3) A 7. alcím, a 19. §, a 20. §, a 22. § (1) bekezdése, a 23. § (1), (4), (6), (7), (11) és (12) bekezdése, a 26. §, a 28. § (3) bekezdés *d), f)* és *h)* pontja, a 28. § (5) és (6) bekezdése, a 30. § (1), (2), (4) és (5) bekezdése, a 40. §, a 42. §, a 48. §, valamint az 1. és a 2. melléklet 2024. január 1-jén lép hatályba.

(4) A 21. §, a 22. § (2)–(9) bekezdése, a 23. § (2), (3), (5), (8)–(10) és (13) bekezdése, a 24. §, a 25. §, a 10. alcím, a 28. § (1) bekezdés *e)–g)* pontja, a 28. § (3) bekezdés *e), g), i)* és *j)* pontja, a 30. § (3) bekezdése, a 33–37. §, a 38. § *a)* és *c)* pontja, a 46. § és a 49. § 2024. október 18-án lép hatályba.

13. Átmeneti rendelkezések

30. § (1)
(2)
(3)
(4)
(5)

14. Az Alaptörvény sarkalatosságra vonatkozó követelményének való megfelelés

31. § A 39–42. §, a 47–49. § és az 51. § az Alaptörvény 23. cikke alapján sarkalatosnak minősül.

15. Az Európai Unió jogának való megfelelés

32. § (1) Ez a törvény az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) szóló, 2019. április

17-i (EU) 2019/881 európai parlamenti és tanácsi rendelet végrehajtásához szükséges rendelkezéseket állapít meg.

(2) Ez a törvény az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

16. Módosító rendelkezések

33–37. §

38. § Hatályát veszti az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

a)

b)

c)

d)–k)

39. §

40. §

41. §

42. §

43–45. §

46. §

47. §

48. §

49. §

50–51. §

1–2. melléklet a 2023. évi XXIII. törvényhez